

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-124178

(43)Date of publication of application : 06.05.1994

(51)Int.Cl.

G06F 3/12

B41J 2/485

B41J 5/30

G06F 12/14

(21)Application number : 04-300383

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 13.10.1992

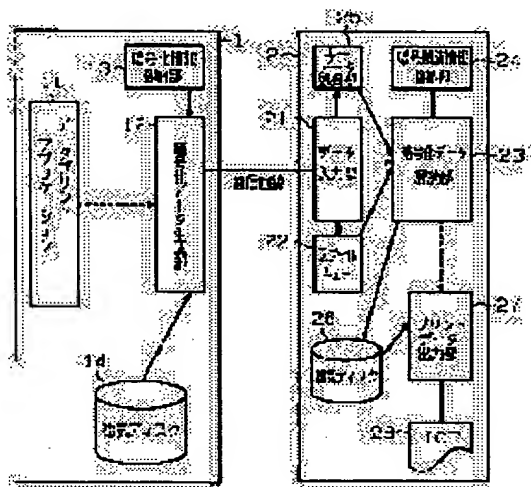
(72)Inventor : YOMOGIZAWA MITSUHISA

(54) SECURITY SYSTEM FOR PRINT DATA

(57)Abstract:

PURPOSE: To exactly ensure security by preventing the content of security objective data existing in a spool queue from being known even when the third person tries to look in at the security objective data through a display or the like.

CONSTITUTION: A print data preparing device 1 is equipped with a ciphered data preparing part 12 which ciphers print data, adds a user ID, key code, and ciphered ID to the ciphered data, and transfers the data to a printer side. A printer 2 is equipped with a ciphered data deciphering part 23 which decipheres the ciphered data based on the user ID or the like. The ciphered data transferred to the printer 2 are temporarily stored in a spool queue 22, and at the time of printing, the ciphered data are deciphered by the ciphered data deciphering part 23, and outputted, only when a password is matched. The ciphered data are stored in the spool queue 22, so that only the lump of the meaningless data can be seen even when the third person tries to look in at the content, and the content of the print data can be prevented from being known.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)特許出願公開番号

特開平6-124178

(43)公開日 平成6年(1994)5月6日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 3/12	A			
B 4 1 J 2/485				
5/30	Z	8703-2C		
G 0 6 F 12/14	3 2 0 B	9293-5B		
		8703-2C		
			B 4 1 J 3/12	Z
			審査請求 未請求 請求項の数1(全 9 頁)	

(21)出願番号 特願平4-300383

(22)出願日 平成4年(1992)10月13日

(71)出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂三丁目3番5号

(72)発明者 蓬沢 光久

埼玉県岩槻市府内3丁目7番1号 富士ゼ

ロックス株式会社内

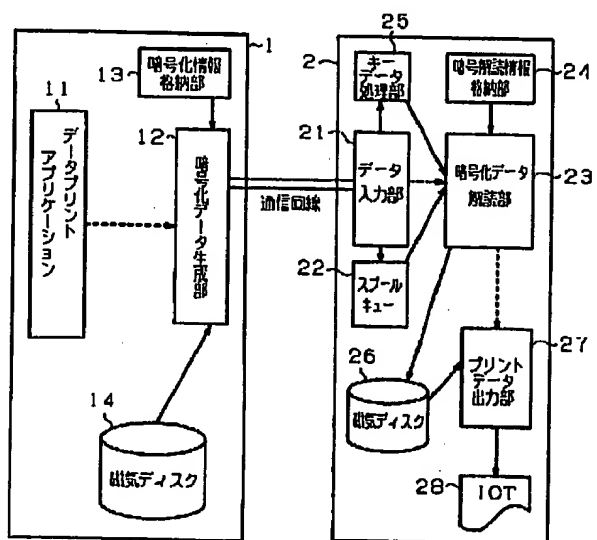
(74)代理人 弁理士 本庄 富雄 (外1名)

(54)【発明の名称】 プリントデータのセキュリティ方式

(57)【要約】

【目的】 スプールキューにセキュリティ対象データが存在していて、第三者がそれをディスプレイ等を通して覗き見しようとしても、その内容を知られないようにして、セキュリティを確実に保つこと。

【構成】 プリントデータ生成装置1には、プリントデータを暗号化すると共に、暗号化データにユーザID、キーコード、暗号化IDを付加してプリンタ側に転送する暗号化データ生成部12を設ける。プリンタ2には、上記ユーザID等に基づいて、上記暗号化データを解読する暗号化データ解読部23を設ける。プリンタ2に転送された暗号化データは、一旦スプールキュー22に格納され、プリントする際には、パスワードが一致した時のみ、暗号化データ解読部23で暗号解読しながら出力する。スプールキュー22に格納されるのは、暗号化データであるので、その内容を覗き見されたとしても、見えるのは意味のないデータの塊であり、プリントデータの内容は知られずに済む。



【特許請求の範囲】

【請求項1】 プリントデータ生成装置は、プリントデータを暗号化すると共に、暗号化したプリントデータにユーザID、キーコード、暗号化IDを付加してプリンタに転送する暗号化データ生成部を有し、プリンタは、転送された暗号化データを格納するスプールキューと、パスワードの一致を確認した上で上記スプールキューから暗号化データを取り出し、それを上記ユーザID、キーコード、暗号化IDに基づいて解読し、解読したデータをプリントデータ出力側に送る暗号化データ解読部を有することを特徴とするプリントデータのセキュリティ方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、プリンティングシステムにおけるプリントデータのセキュリティ方式に関するものである。

【0002】

【従来の技術】図10は、ネットワークにホストコンピュータ及びプリンタが接続された状態を示す図である。図10において、100はネットワーク、101～105はプリンタ、111～113はホストコンピュータである。プリンタ101～105は、ネットワーク100に接続され、そのネットワーク100に接続された複数のホストコンピュータ111～113からの出力データを印刷する。

【0003】このようにプリンタが複数の利用者と共用される場合、そのまま外部に出力させるのではプリントされた出力データが第三者の目に触れる可能性があり、機密が保持できない。そのため、機密を保持できるような対策を施したプリントデータのセキュリティ方式が従来から提案されている。従来の一般的なプリントデータのセキュリティ方式では、プリンタに対して、通常のプリントデータをパスワード付で転送する。プリンタ側では、転送されてきたプリントデータをパスワードと共にスプールキューに保持しておく。そして、それをプリントする際には、操作者に対してパスワードを要求し、入力されたパスワードと保持しておいたパスワードとが一致したときのみプリントを実行するようにして、セキュリティを確保するようにしている。

【0004】なお、このようなプリントデータのセキュリティ方式に関連する従来の文献としては、例えば、特開昭61-269729号公報、特開昭62-3322号公報、特開平1-159724号公報等がある。

【0005】

【発明が解決しようとする課題】

（問題点）しかしながら、前記した従来の技術には、スプールキュー内にプリントデータが存在する場合、第三者がディスプレイ等を通してその内容を見ることができ、データの機密を確実に保持することはできないとい

う問題点があった。

【0006】（問題点の説明）従来の方式では、パスワードを知っていない限り、そのデータをプリントすることはできないが、プリントデータ自体は通常のデータである。したがって、それがスプールキュー内に保持されている時、見ようと思えば、プリンタに接続されているディスプレイを通してデータの中身を見ることは可能である。そのため、データの機密を確実に保持できない。本発明は、以上のような問題点を解決することを課題とするものである。

【0007】

【課題を解決するための手段】前記課題を解決するため、本発明のプリントデータのセキュリティ方式では、プリントデータ生成装置は、プリントデータを暗号化すると共に、暗号化したプリントデータにユーザID、キーコード、暗号化IDを付加してプリンタに転送する暗号化データ生成部を有し、プリンタは、転送された暗号化データを格納するスプールキューと、パスワードの一致を確認した上で上記スプールキューから暗号化データを取り出し、それを上記ユーザID、キーコード、暗号化IDに基づいて解読し、解読したデータをプリントデータ出力側に送る暗号化データ解読部を設けることとした。

【0008】

【作 用】プリントデータ生成装置の暗号化データ生成部で、プリントデータは全て暗号化してからプリンタ側に転送する。一方、プリンタ側では、プリント出力するのはパスワードの一致を確認してからであるので、第三者がプリント出力するのを防止することができる。その上、暗号化されたプリントデータが解読されるのは、プリント出力する時であり、スプールキューには、転送されてきたデータがそのままの形で格納される。そのため、スプールキューにセキュリティ対象データが存在していても、そのデータは全て暗号化されていて、それをディスプレイ等を通して見ようとしても、見えるのは何の意味も持たないデータの塊であり、第三者にその内容を知られることはない。したがって、データの機密が確実に保持できる。

【0009】

【実施例】以下、本発明の実施例を図面に基いて詳細に説明する。図1は、本発明の概要を示すブロック図である。図1において、1はプリントデータ生成装置、11はデータプリントアプリケーション、12は暗号化データ生成部、13は暗号化情報格納部、14は磁気ディスク、2はプリンタ、21はデータ入力部、22はスプールキュー、23は暗号化データ解読部、24は暗号解読情報格納部、25はキーデータ処理部、26は磁気ディスク、27はプリントデータ出力部、28は記録部である。

【0010】プリントデータ生成装置1は、ホストコン

ピュータ、ワークステーション、パーソナルコンピュータ、ワードプロセッサ等の、プリントデータを生成する機能を有する装置である。生成されたプリントデータは、一旦磁気ディスク14に格納される。データプリントアプリケーション11は、暗号化データ生成部12を起動させ、磁気ディスク14に格納されているプリントデータの内、どのデータを処理するかを指示する。暗号化データ生成部12は、暗号化情報格納部13に格納されているキーコード、暗号化ID、暗号化手法等に基づいて、磁気ディスク14に格納されているプリントデータを暗号化して、プリンタ2に転送する。

【0011】プリンタ2のデータ入力部21は、プリントデータ生成装置1から転送されたデータの内、暗号化データをスプールキュー22に格納する。キーデータ処理部25は、転送されたデータから、ユーザID、暗号化ID、キーコードを抜き出して保持する。暗号化データ解読部23は、スプールキュー22から暗号化データを受け取り、キーデータ処理部25からそれに対応するユーザID、暗号化ID、キーコードを受け取り、さらに、暗号解読情報格納部24から暗号解読手法等の暗号解読情報を受け取って、暗号化データを解読する。磁気ディスク26は、解読された後のプリントデータを一時保持した後、プリントデータ出力部27に引き渡す。

【0012】図2は、暗号化情報格納部に格納されたデータの一例を示す図である。図2(イ)は、キーコード、暗号化ID格納テーブルであり、各ユーザID毎に、使用されるキーコードと暗号化IDとを、それぞれ複数個ずつ格納している。図2(ロ)は、暗号化手法格納テーブルであり、各暗号化IDに対応する暗号化手法を格納している。

【0013】図3は、暗号解読情報格納部に格納されたデータの一例を示す図である。図3(イ)は、セキュリティ対象ユーザID格納部であり、プリントデータの機密を保持する必要があるユーザのユーザIDを格納している。図3(ロ)は、ユーザID格納テーブルであり、各ログオンクラス毎に、そのログオンクラスでのプリント出力が許されるユーザのユーザIDを格納している。図3(ハ)は、暗号解読手法格納テーブルであり、各暗号化IDに対応する暗号解読手法を格納している。これらの暗号解読手法は、図2(ロ)の暗号化手法格納テーブルに格納されている暗号化手法と1対1に対応している。なお、上記「ログオンクラス」とは、プリンタを操作する際にアクセスできるファイルや起動できるプログラムを、ユーザに応じて区別するためのものであり、通常、上位のログオンクラスに指定されたユーザほどアクセスできるファイルや起動できるプログラムの数は多くなる。

【0014】次に、プリントデータ生成装置1からプリンタ2に転送するデータの内容を説明する。図4は、本発明による転送データフォーマットの一例を示す図であ

る。このデータは、プリントデータ生成装置1の暗号化データ生成部12で生成されるが、暗号化データにユーザID、暗号化ID、キーコードが付加される。

【0015】次に、本発明の動作をフローチャートを参照しながら説明する。なお、プリントデータ生成装置1における暗号化情報格納部13、及び、プリンタ2における暗号解読情報格納部24の各データは、予め設定されているものとする。まず、プリントデータ生成装置1の暗号化データ生成部12において、プリントデータを暗号化してプリンタ2に転送する手順を説明する。

【0016】図5は、プリントデータを暗号化して転送する手順の一例を示すフローチャートである。

ステップ1…ユーザが入力したユーザIDを転送データのAの箇所(図4参照。以下、同様)にセットする。

ステップ2…暗号化情報格納部13のキーコード、暗号化ID格納テーブル(図2(イ)参照)中の上記ユーザIDに対応する複数のキーコードの中から、1つをランダムに選定して、転送データのCの箇所にセットする。

ステップ3…暗号化情報格納部13のキーコード、暗号化ID格納テーブル(同上)中の上記ユーザIDに対応する複数の暗号化IDの中から、1つをランダムに選定して、転送データのBの箇所にセットする。

【0017】ステップ4…データプリントアプリケーション11によって指定されたプリントデータを、磁気ディスク14から読み込む。

ステップ5…暗号化情報格納部13の暗号化手法格納テーブル(図2(ロ)参照)中の、ステップ3で選定した暗号化IDに対応する暗号化手法に基づいて、プリントデータの暗号化を行う。

ステップ6…暗号化データを転送データのDの箇所にセットして、データをプリンタ2に転送する。

【0018】次に、プリンタ2の暗号化データ解読部23において、暗号化データを解読してプリントを開始させる手順を説明する。この手順は、プリント出力させようとする操作者が、プリントするデータ及びログオンクラスを指定してから開始される。図6は、暗号化データを解読してプリントを開始させる手順の一例を示すフローチャートである。

ステップ1…キーデータ処理部25から、プリントするデータに対応するユーザIDを取得する。

ステップ2…暗号解読情報格納部24のユーザID格納テーブル(図3(ロ)参照)中の、操作者が指定したログオンクラスに対応するユーザIDの中にステップ1で取得したユーザIDが有るか否かを調べる。

ステップ3…ない時、そのユーザに対して当該ログオンクラスでのプリントが許可されていないということになる。そこで、ログオンクラスの変更を促すメッセージをプリンタに接続されているディスプレイに表示し、入力を待つ。

ステップ4…暗号解読情報格納部24のユーザID格納

テーブル(同上)中の、変更されたログオンクラスに対応するユーザIDの中にステップ1で取得したユーザIDが有るか否かを調べる。

ステップ5…ない時、変更されたログオンクラスでもプリントが許可されていないということになる。その時は、プリンタに接続されているディスプレイにエラー表示をして、プリントすることなく処理を終了する。

【0019】ステップ6…ステップ2、ステップ4でユーザIDがあった時、暗号解読情報格納部24のセキュリティ対象ユーザID格納部(図3(イ)参照)の中に
10 ステップ1で取得したユーザIDが有るか否かを調べる。

ステップ7…あれば、プリントデータの機密を保持する必要があるということになる。そこで、現在プリントしようとしている操作者がプリントデータを送ってきたユーザ本人であるか否かを確認するため、操作者に対してパスワードの入力を促すメッセージをプリンタに接続されているディスプレイに表示し、入力を待つ。

ステップ8…入力されたパスワードが予め登録されていたものと一致したか否かを判別する。

ステップ9…一致したら、キーデータ処理部25から暗号化IDを取得する。

ステップ10…続いて、キーデータ処理部25からキーコードを取得する。

ステップ11…暗号解読情報格納部24の暗号解読手法格納テーブル(図3(ハ)参照)から、ステップ9で取得した暗号化IDに対応する暗号解読手法を取得する。

ステップ12…暗号化データの解読を行う。

ステップ13…解読したプリントデータを磁気ディスク26を介してプリントデータ出力部27に送って、
30 プリントを開始させる。

【0020】このようにすれば、先ず、パスワードによって、第三者がプリント出力するのを防止することができる。その上、スプールキューに格納されるデータは暗号化データであるので、スプールキューにセキュリティデータが存在していても、そのデータは全て暗号化されていて、それをディスプレイ等を通して見ようとしても、見えるのは何の意味も持たないデータの塊であり、第三者にその内容を知られる恐れはない。その結果、データの機密が確実に保持される。また、パスワードだけでなく、ログオンクラスとの組合せによりプリント出力の可否を判定するようにしているため、より高度のセキュリティを確保できる。さらに、暗号化手法及びキーコードを複数の中からランダムに1つを選定するようにしているため、同じデータの暗号化でも1回目と2回目の暗号化データが同一になる確率は低くなり、データの隠蔽がより高度なものとなる。

【0021】上記実施例では、ステップ4で、ログオンクラスが変更されても、それに対応するユーザIDの中に
50 ステップ1で取得したユーザIDがなかった時、ある

いは、ステップ8で、パスワードが一致しなかった時、エラー表示を行って、プリントはしないようにしていた。しかし、そのような時、エラー表示を行うことなく、暗号化されたデータをそのまま印刷するようにすることもできる。図7は、暗号化データを解読してプリントを開始させる手順の他の例を示すフローチャートである。このフローチャートは、ステップ4、ステップ7でNOと判定された時、図6のフローチャートにおけるステップ5(エラー表示)を省略し、ステップ12(プリント開始)を実行するようにしている点だけが、図6のものとは相違しており、その他の手順は同じである。このようにすれば、例えば、パスワードが一致しなくてもプリントは実行されるが、暗号解読が行われなままプリント出力されるため、出力されるデータは意味不明のものとなり、プリントデータの機密は保持される。

【0022】以上の実施例では、転送データフォーマット中のユーザIDは、個人に対応するものであった。しかし、それをグループに対応させて取り扱うようにすることもできる。図8は、暗号化情報格納部に格納されたデータの他の例を示す図であり、図9は、暗号解読情報格納部に格納されたデータの他の例を示す図である。図8(イ)は、グループユーザID格納テーブルであり、各グループユーザID毎に、そのグループに属するユーザIDが格納されている。図8(ロ)、図8(ハ)は、図2(イ)、図2(ロ)と同様なテーブルである。また、図9(イ)、図9(ロ)、図9(ハ)は、図3(イ)、図3(ロ)、図3(ハ)と同様な内容であるが、ただ、図9(ロ)のユーザID格納テーブルの中に、ユーザIDと共に、グループユーザIDも設定されている点で異なっている。

【0023】すなわち、図8、図9のものが、図2、図3のものと異なる点は、プリントデータ生成装置1側において、複数のユーザIDに対して、グループユーザIDを定義する点である。また、プリンタ2側においても、各ログオンクラスにて、グループユーザIDの設定も行っている点である。

【0024】この場合、プリントデータ生成装置1において、処理を行う際に入力するIDとしては、やはりユーザIDを入力する。ユーザIDが入力されると、図8(イ)のグループユーザID格納テーブルに基づいて、当該ユーザが属するグループユーザIDが取得される。そして、転送データのAの箇所(図4参照)には、そのグループユーザIDがセットされる。転送データのB、Cの箇所には、それぞれ、ユーザIDに対応する暗号化ID及びキーコードがセットされる。プリンタ2側において暗号解読を行うに際しては、グループユーザIDは、ユーザIDと同等に取り扱われる。

【0025】また、図10に示したように、ネットワーク上に複数のホストコンピュータ111~113とプリンタ101~105が接続されている場合に、ユーザI

Dの代わりに、各ホストコンピュータのマシンIDを用いて、ホストコンピュータ単位でのプリント可否を設定することもできる。その場合、必ずしも、ホストコンピュータとマシンIDとが1対1に対応する必要はなく、複数のホストコンピュータに対して、1つのマシンIDを与えるようにしても差し支えない。

【0026】

【発明の効果】以上述べた如く、本発明のプリントデータのセキュリティ方式によれば、次のような効果を奏する。まず、パスワードによって、第三者がプリント出力するのを防止することができる。その上、スプールキューに格納されるデータは暗号化データであるので、スプールキューにセキュリティデータが存在していても、そのデータは全て暗号化されていて、それをディスプレイ等を通して見ようとしても、第三者にその内容を知られる恐れはなく、データの機密が確実に保持される。また、実施例で行ったように、パスワードだけでなく、ログオンクラスとの組合せによりプリント出力の可否を判定するようにすれば、より高度のセキュリティを確保できる。さらに、暗号化手法及びキーコードを複数の中からランダムに1つを選定するようにすれば、同じデータの暗号化でも1回目と2回目の暗号化データが同一になる確率は低くなり、データの隠蔽がより高度なものとなる。

【図面の簡単な説明】

【図1】 本発明の概要を示すブロック図

【図2】 暗号化情報格納部に格納されたデータの一例*

*を示す図

【図3】 暗号解読情報格納部に格納されたデータの一例を示す図

【図4】 本発明による転送データフォーマットの一例を示す図

【図5】 プリントデータを暗号化して転送する手順の一例を示すフローチャート

【図6】 暗号化データを解読してプリントを開始させる手順の一例を示すフローチャート

10 【図7】 暗号化データを解読してプリントを開始させる手順の他の例を示すフローチャート

【図8】 暗号化情報格納部に格納されたデータの他の例を示す図

【図9】 暗号解読情報格納部に格納されたデータの他の例を示す図

【図10】 ネットワークにホストコンピュータ及びプリンタが接続された状態を示す図

【符号の説明】

1…プリントデータ生成装置、11…データプリントアプリケーション、12…暗号化データ生成部、13…暗号化情報格納部、14…磁気ディスク、2…プリンタ、21…データ入力部、22…スプールキュー、23…暗号化データ解読部、24…暗号解読情報格納部、25…キーデータ処理部、26…磁気ディスク、27…プリントデータ出力部、28…記録部、100…ネットワーク、101～105…プリンタ、111～113…ホストコンピュータ

【図2】

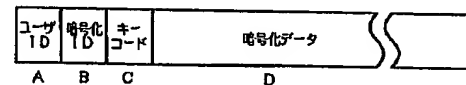
	ユーザID	キーコード	暗号化ID
1	ID ₁	K ₁ , K ₂ , K ₃	1, 3, 5
2	ID ₂	K ₄ , K ₅ , K ₆	2, 4
3	ID ₃	K ₇ , K ₈ , K ₉	2, 3, 4
⋮	⋮	⋮	⋮
n	ID _n	K ₁₀ , K ₁₁ , K ₁₂	1, 3

(イ)

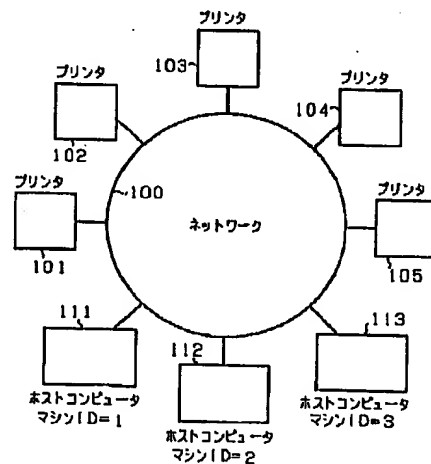
暗号化ID	暗号化手法
1	手法1
2	手法2
3	手法3
4	手法4
5	手法5

(ロ)

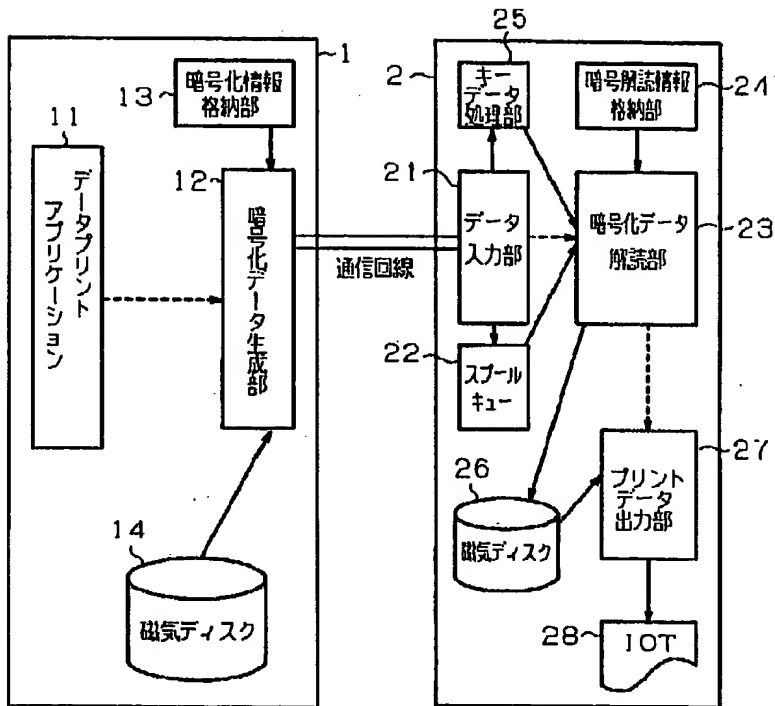
【図4】



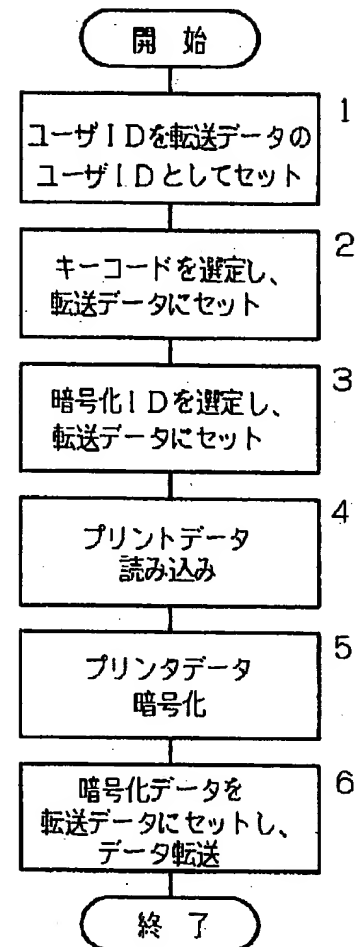
【図10】



【図1】



【図5】



【図3】

セキュリティ対象 ユーザID
ID ₁ , ID ₂ , ID ₄ , ID ₇

(イ)

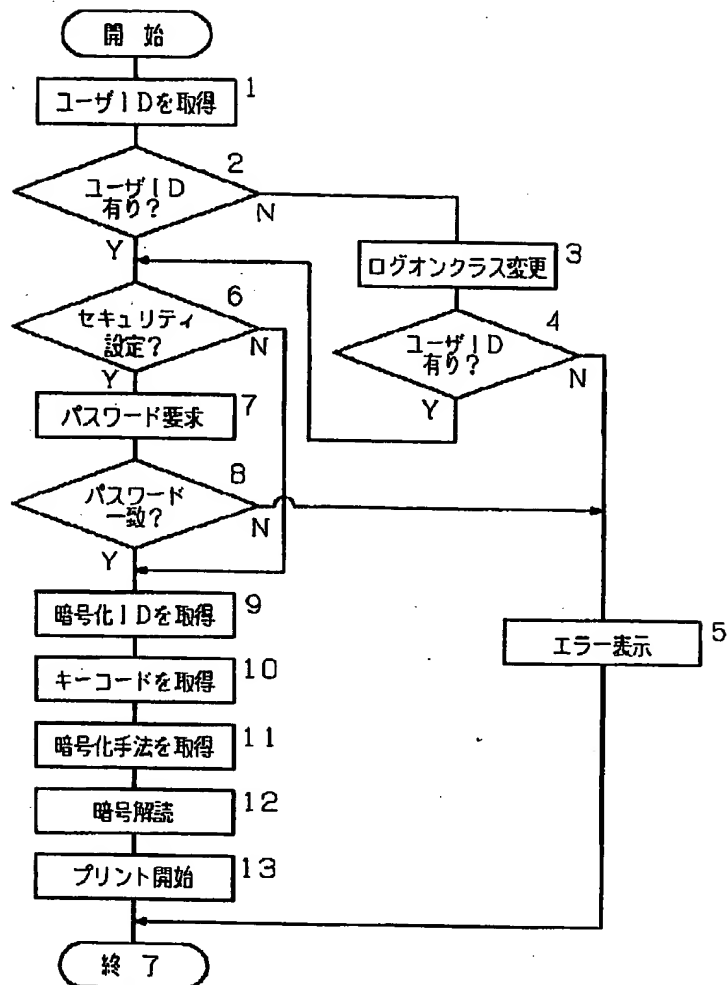
ログイン クラス	ユーザID
1	ID ₁ , ID ₂ , ID ₃
2	ID ₄ , ID ₅
3	ID ₆ , ID ₇
⋮	⋮
N	ID _n

(ロ)

暗号化ID	暗号解読手法
1	解読手法 1
2	解読手法 2
3	解読手法 3
4	解読手法 4
5	解読手法 5

(ハ)

【図6】



【図9】

セキュリティ対象 ユーザID
ID ₁ , ID ₂ , ID ₄ , G I ₂

(イ)

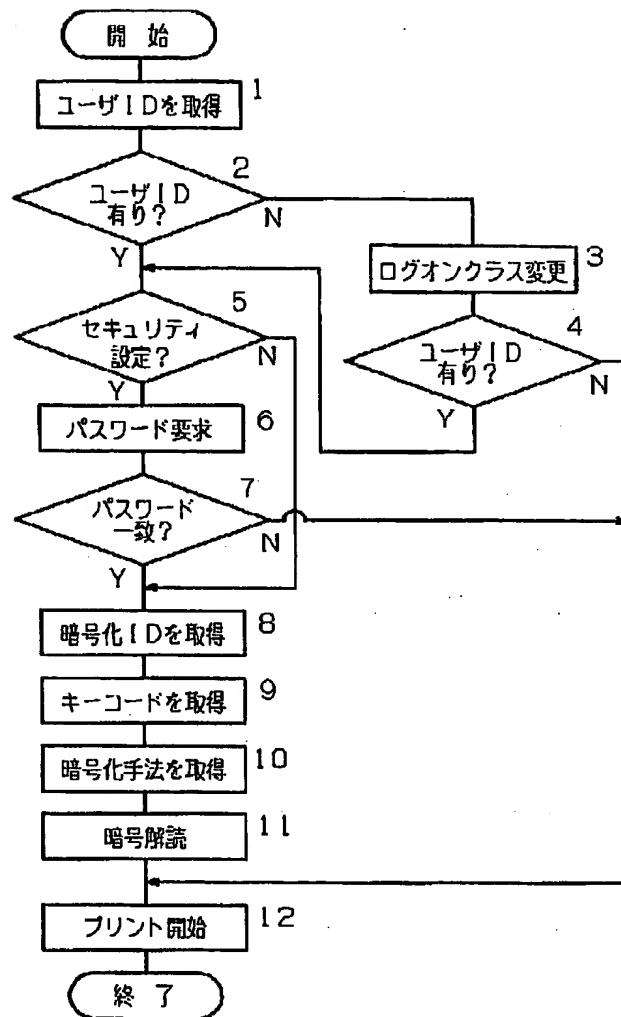
ログオン クラス	ユーザID
1	ID ₁ , ID ₂ , ID ₉
2	ID ₄ , ID ₅
3	G I ₁
4	G I ₂
⋮	⋮
N	ID _n

(ロ)

暗号化ID	暗号解読手法
1	解読手法 1
2	解読手法 2
3	解読手法 3
4	解読手法 4
5	解読手法 5

(ハ)

【図7】



(9)

特開平6-124178

【図8】

	グループユーザID	ユーザID
1	G1 ₁	ID ₁ , ID ₂ , ID ₃
2	G1 ₂	ID ₄ , ID ₅ , ID ₆
⋮	⋮	⋮
L	G1 _L	⋯, ID _L

(イ)

	ユーザID	キーコード	暗号化ID
1	ID ₁	K ₁ , K ₂ , K ₃	1, 3, 5
2	ID ₂	K ₄ , K ₅ , K ₆	2, 4
3	ID ₃	K ₇ , K ₈ , K ₉	2, 3, 4
⋮	⋮	⋮	⋮
n	ID _n	K ₁₀ , K ₁₁ , K ₁₂	1, 3

(ロ)

暗号化ID	暗号化手法
1	手法1
2	手法2
3	手法3
4	手法4
5	手法5

(ハ)